**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | |
| | ) | Criminal No. 1:11-cr-04 Erie |
| v. | ) | (Civ. No. 15-249 Erie) |
| | ) | |
| CRAIG ALAN FINLEY, | ) | Judge Mark R. Hornak |
| | ) | |
| Petitioner/Defendant. | ) | |

**OPINION**

**Mark R. Hornak, United States District Judge**

Pending before the Court is Petitioner Craig Alan Finley's *pro se* Motion to Vacate, Set Aside, or Correct a Sentence pursuant to 28 U.S.C. § 2255 (ECF No. 115) ("Petition") filed at Criminal No. 11-04 (Erie) and as Civil Action No. 15-249 (Erie). The United States has filed a Response to the Motion, to which Mr. Finley has filed a Reply. For the reasons which follow, the Motion will be denied.

## I. BACKGROUND

Mr. Finley was charged in a four-count superseding Indictment with (1) sexual exploitation of a minor in and around August 2010, in violation of 18 U.S.C. §§ 2251(a) and (e); (2) receipt of material depicting the sexual exploitation of a minor from in and around August 2010 to in and around December 2010, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); (3) distribution of material depicting the sexual exploitation of a minor from in and around August 2010 to in and around December 2010, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); and (4) possession of material depicting the sexual exploitation of a minor from in and around August 2010 to in and around December 2010, in violation of §§ 2252(a)(4)(B) and (b)(2). (ECF No. 26).

The charges arose out of a Federal Bureau of Investigation ("FBI") undercover operation on the peer-to-peer Internet file sharing network GigaTribe. GigaTribe is a program offered for free that anyone who has Internet access can download onto their computer. "Peer-to-peer" simply means that the GigaTribe program allows computers in different locations to connect together over the Internet, and GigaTribe will act as a conduit between the computers to allow them to share information and otherwise communicate with one another. GigaTribe allows users to share: (i) only content the user has specifically designated for sharing on GigaTribe; (ii) only with other GigaTribe users that are "friends;" and (iii) only while both users are connected to GigaTribe through the Internet. The FBI undercover agents involved in this case operated on the GigaTribe network using actual GigaTribe usernames that had been taken over by the FBI in prior child pornography operations.

The undercover investigation initially involved FBI Agent Marc Botello of Los Angeles, California communicating via GigaTribe with Mr. Finley in October, 2012. Working independently from Agent Botello, FBI Agent Barry Couch of Rochester, New York communicated via GigaTribe with Mr. Finley in late December, 2012.

On October 21, 2010, Agent Botello logged onto the GigaTribe network using the GigaTribe username, "JoePeter94." Tr., Jan 19, 2012, at 37 (ECF No. 104). He saw the username "Boys4me2010," surveyed his online GigaTribe shared folders, and realizing that a password was required in order to view the contents of the folders, he initiated a chat. *Id.* at 38. When one logs onto GigaTribe, they have to manually set certain files on the computer to share, that is, one has to affirmatively make the content available for others to download *Id.* at 16. Botello asked Boys4me2010 if he (Botello) could have the password for a folder titled "stuff" that Boys4me2010 was sharing on the network. *Id.* at 39, 46. Boys4me2010 gave Botello the

password. *Id.* at 46. Botello clicked on the folder, entered the password, and the list of files the folder contained was displayed to Botello. *Id.* at 51. Botello then downloaded several files from the "stuff" folder verifying that they contained what appeared to be child pornography. *Id.* at 52-54.

Botello was able to identify username Boys4me2010 as operating from an IP address of 72.23.47.145 on October 21, 2010. *Id.* at 45, 54. He further confirmed that IP address of 72.23.47.145 was registered with Armstrong Cable Services of Butler, Pennsylvania. *Id.* at 60. Botello served Armstrong Cable with a request for the subscriber information for the IP address 72.23.47.145. *Id.* On November 2, 2010, Armstrong Cable responded that the subscriber was Craig Alan Finley with a residence address in Titusville, Pennsylvania. *Id.* at 61-65. Botello passed the information he had gathered about Boys4me2010 onto the FBI field office in Erie, Pennsylvania because that office covers the Titusville, Pennsylvania area. *Id.* at 65-66.

Erie FBI Agent Michael Shaffer received the lead from Agent Botello in early December, 2010, and began initial preparation and investigation towards gaining a search warrant for Mr. Finley's residence. Tr. Jan. 24, 2012, at 3 (ECF No. 105). Before a search warrant was obtained, Agent Barry Couch in Rochester, New York, logged onto the GigaTribe network on December 20, 2012, in an undercover capacity using the GigaTribe username "PurpleTrim420." Tr., Jan 19, 2012, at 88-89 (ECF No. 104). Because PurpleTrim420 was at one time an active account trading child pornography, the user had a friends' list that included Boys4me2010. *Id.* at 91. Couch engaged in a conversation with Boys4me2010. *Id.* at 91, 96. He pretended that he had forgotten Boys4me2010's passwords for his shared GigaTribe folders and asked for them again. *Id.* at 96. Boys4me2010 gave Couch the passwords. *Id.* at 97-98. Couch then used the passwords to unlock the Boys4me2010's shared folders and downloaded several still images and

movies of child pornography. *Id.* at 98-104. Couch viewed information that user Boys4me2010 had placed in his profile, which indicated that the user was a male with a birthdate of January 26, 1977.

Couch continued chatting with Boys4me2010 and learned that the user may be physically engaged in sexual conduct with a minor child. *Id.* at 106. Because there was potentially a victim in present danger of being molested, Couch continued chatting with Boys4me2010 in order to learn as much information as he could to allow law enforcement to take steps to protect the potential victim. *Id.* at 107-18. Through his conversation with Boys4me2010, Couch learned that the user was approximately 33 years old; the minor children were boys ranging in age from 7 to 14 years old; the minor boys were related to the user; the user did not own a vehicle and he lived within a 15-minute walking distance of the minors. *Id.* at 119-22.

Couch served Armstrong Cable with a request for the subscriber information for the IP address 72.23.47.145 being used on December 20, 2012. *Id.* at 130. Armstrong Cable Company responded that the IP address was registered to Craig Finley with a residence address in Titusville, Pennsylvania. *Id.* at 131. Couch then forwarded the information he had gathered to the Erie FBI field office, letting the office know that there was an immediate concern that an adult might be engaging in sexual conduct with a minor. *Id.* at 132.

Agent Shaffer was already preparing for a search warrant for Mr. Finley's residence based on the information Botello had forwarded to him in early December when the second lead from Couch came in containing the identical IP address and GigaTribe username. Tr. Jan. 24, 2012, at 4 (ECF No. 105). The matter became a priority for Couch because of the allegation that a minor child was at risk, and thus the FBI obtained and executed a search warrant on December 23, 2010. *Id.* at 4-5.

On the day the search warrant was executed, Couch logged onto GigaTribe and was able to see that Boys4me2010 was also logged into his GigaTribe account. *Id.* at 8-9. Couch shared this information with Shaffer, and so he proceeded to Mr. Finley's residence assuming that Mr. Finley was at home. *Id.* at 9. The Agents knocked at the door and announced that it was law enforcement. *Id.* When no one answered, the Agents decided to forcefully enter the apartment believing Mr. Finley may be attempting to destroy evidence. *Id.* When the Agents entered the apartment they discovered that Mr. Finley was not there. *Id.*

Agent Shaffer viewed Mr. Finley's running computer. *Id.* at 10. The screen on the monitor was asleep. *Id.* at 16. Shaffer moved the mouse connected to the computer tied to the sleeping monitor, which "woke up" the screen. *Id.* at 13, 16. Viewing the screen, Agent Shaffer confirmed that the GigaTribe program with a username of Boys4me2010 was active on the computer. *Id.* at 13-14, 16. Prior to the search, Shaffer had viewed an image that Couch had downloaded that Boys4me2010 was sharing on GigaTribe of a boy sitting on a green couch, and further observed the same green couch in Mr. Finley's apartment. *Id.* at 17-18.

Assisting with the execution of the search warrant were Titusville police officers who knew that Mr. Finley's brother lived close by. Tr. Jan. 17, 2012, at 29 (ECF No. 102). The Agents decided to go to Mr. Finley's brother's house thinking that Mr. Finley might be there. *Id.*; Tr. Jan. 24, 2012, at 22. He was not. Tr. Jan. 17, 2012, at 30. The officers were told that he was Christmas shopping with his sister-in-law. *Id.* One of the occupants called the sister-in-law and handed the phone to an Agent who spoke with her, and then with Mr. Finley. *Id.* The Agent asked him to return to his apartment. After he arrived, Mr. Finley was interviewed, and the search warrant process was completed. Among the items seized from Mr. Finley's apartment

were two computers (one computer was not plugged in) and a cell phone that Mr. Finley possessed when he was searched.

Pennsylvania State Police Corporal Robert Pearson examined the two computers and the cell phone seized during the execution of the search warrant. Tr. Jan. 24, 2012, at 51 (ECF No. 105). He is a federally deputized law enforcement officer and expert in computer forensics. *Id.* at 37-38. At the time of trial he was the coordinator of the Northwest Computer Crimes Task Force. *Id.* at 37. His examination showed that both computers contained, among other items, Mr. Finley's resume, a link to his Facebook page, a GigaTribe account for Boys4me2010, a Skype account with the username Boys4me2010, an AOL account with the username Boys4me2010, and over 30,000 images and videos of child pornography. *Id.* at 58-65. Corporal Pearson discovered multiple saved chat logs showing that Boys4me2010 had engaged in conversations with 100's of other GigaTribe users about sharing, distributing, and receiving child pornography. *Id.* at 74-110. A review of the chat records revealed that on October 3, 2010, Boys4me2010 announced to other GigaTribe users that he was updating his GigaTribe folders as a result of a computer change. *Id.* 109-110, 121. In addition, the chat records indicated numerous instances when Boys4me2010 tells other GigaTribe users that he leaves his computer and GigaTribe account up and running when he is away from his computer. *Id.* at 142-44.

Mr. Finley was arrested and detained on December 23, 2010. Assistant Federal Public Defender Thomas Patton was appointed to represent Mr. Finley. A jury trial was set for January, 2012. On December 14, 2011, Mr. Patton filed a motion to suppress statements Mr. Finley gave to the Agents when he was questioned at his apartment. On January 4, 2012, Mr. Finley sent a letter to the Court, which was filed as a motion to disqualify counsel.

The Court held a hearing on the motion to disqualify counsel on January 10, 2012. Tr. Jan. 10, 2012 (ECF No. 92). The Court conducted an *in camera* examination of Mr. Finley outside of the presence of both the government and Mr. Patton. *Id.* at 4-10. Mr. Finley explained that he no longer wanted Mr. Patton to represent him because of communication issues, disagreements about trial strategy, pressure to take a plea, non-response to requests to file motions, and refusal to file motions. *Id.* at 4-8. The Court told Mr. Finley that it was "not going to replace him based on what you have told me this morning. I just don't think there's a good basis for that, granting that request." *Id.* at 9.

In open court the Court asked Mr. Patton questions regarding his relationship with Mr. Finley, his ability to represent Mr. Finley, and whether he pressured him to take a plea. *Id.* at 10-11. Being satisfied that Mr. Patton was able to properly represent Mr. Finley, the Court denied Mr. Finley's motion to disqualify counsel and his request to continue the trial to seek new counsel. *Id.* at 11.

A suppression hearing was held prior to trial on January 17, 2012. Tr. Jan. 17, 2012 (ECF No. 102). After testimony and evidence were received, the Court found that Mr. Finley was in custody at the time he was questioned and that he had not been given *Miranda* warnings. Accordingly, the motion to suppress was granted and Mr. Finley's statements were ruled inadmissible.

A jury trial began on January 18, 2012, after which Mr. Finley was convicted of all four counts. Prior to sentencing the Court issued tentative findings and rulings finding that (i) a vulnerable victim enhancement pursuant to U.S.S.G. § 3A1.1(b)(1) was proper because the Court determined that the minor victim was asleep, making the child unusually vulnerable; and (ii) that

no sentence would be imposed at Count 4 of the superseding indictment because it is a lesser included offense of Count 2.

On May 8, 2012, Mr. Finley was sentenced to a total term of imprisonment of 50 years, consisting of 30 years at Count 1 of the superseding indictment, a consecutive 20-year sentence at Count 2 of the superseding indictment, and a concurrent term of 20 years' imprisonment at Count 3 of the superseding indictment.

A timely appeal to the United States Court of Appeals for the Third Circuit was filed by Assistant Federal Public Defender Karen Sirianni Gerlach. On August 12, 2013, that court issued its opinion affirming the judgment of conviction and sentence. *United States v. Finley*, 726 F.3d 483 (3d Cir. 2013). Thereafter, Mr. Finley timely filed his motion to vacate, raising issues as to the claimed ineffectiveness of both his trial and appellate counsel.

## II. STANDARD OF REVIEW

Section 2255 of Title 28 of the United States Code provides a means of collaterally attacking a sentence imposed after a conviction. *See United States v. Cannistraro*, 734 F. Supp. 1110, 1119 (D. N.J. 1989), *aff'd sub nom. Appeal of Cannistraro,* 919 F.2d 133 (3d Cir. 1990), and *aff'd* 919 F.2d 137 (3d Cir. 1990). Pursuant to 28 U.S.C. § 2255, a federal prisoner may move the sentencing court to vacate, set aside, or correct a sentence:

> [U]pon the ground that the sentence was imposed in violation of the Constitution or laws of the United States, or that the court was without jurisdiction to impose such sentence, or that the sentence was in excess of the maximum authorized by law, or is otherwise subject to collateral attack.

28 U.S.C. § 2255 (2012). Relief under this provision is "generally available only in 'exceptional circumstances' to protect against a fundamental defect which inherently results in a complete miscarriage of justice or an omission inconsistent with the rudimentary demands of fair

procedure." *United States v. Gordon*, 979 F. Supp. 337, 339 (E.D. Pa. 1997) (*quoting Hill v. United States*, 368 U.S. 424, 428 (1962).

A district court is required to hold an evidentiary hearing on a motion to vacate sentence filed pursuant to 28 U.S.C. § 2255 unless the motion, files, and records of the case show conclusively that the movant is not entitled to relief. *See* 28 U.S.C. § 2255(b); *United States v. Booth*, 432 F.3d 542, 545-46 (3d Cir. 2005); *United States v. Nahodil*, 36 F.3d 323, 326 (3d Cir. 1994). Thus, if the record conclusively negates the factual predicates asserted in support of a § 2255 motion, or if the movant would not be entitled to relief as a matter of law even if the factual predicates as alleged in the motion are true, an evidentiary hearing is not required. *See Government of Virgin Islands v. Nicholas*, 759 F.2d 1073, 1075 (3d Cir. 1985).

The Court finds no need for an evidentiary hearing here, as the record conclusively establishes that Mr. Finley is not entitled to the relief sought in the petition. See 28 U.S.C. § 2255. Accordingly, his motion for an evidentiary hearing will be denied.

## III. DISCUSSION

Mr. Finley argues that he was denied effective assistance of counsel under the Sixth Amendment of the Constitution at trial and on appeal. Underlying Mr. Finley's ineffectiveness of counsel arguments is his central assertion that an anonymous, unauthorized person surreptitiously and illegally accessed his computers, engaged in the numerous chat session with other GigaTribe users, and caused images and videos of child pornography to be placed on his computers.

Specifically, Mr. Finley alleges his counsel was ineffective as follows:

- in failing to challenge the search warrant because the officers had knowledge indicating unauthorized user activity;

- in failing to move for acquittal pretrial, during trial, and post-trial as to Count One because the depiction did not meet the definition of sexual activity nor did the evidence establish Mr. Finley's receipt;

- in refusing to investigate and present an alternate user defense theory;

- in failing to subpoena certain character and fact witnesses;

- in failing to adequately cross-examine government witnesses Shaffer, Couch, Botello, Pearson, and Blashford;

- in failing to object to prosecutorial misconduct;

- in failing to be competent in computer forensics; and

- in failing to preserve issues for appeal.

Mr. Finley also argues that his Sixth Amendment right to effective counsel was violated by the court denying his motion to appoint new counsel because it resulted in "conflicted" counsel as follows:

- trial counsel was "representing conflicting interests," by which Mr. Finley means Mr. Patton refused to investigate Mr. Finley's defense and that Mr. Patton would not vigorously and competently pursue Mr. Finley's defense strategy;

- appellate counsel was ineffective because she was operating under a conflict based on the fact that she was employed by the same Federal Public Defender's office as Mr. Patton, and that she failed to raise any issue based on Mr. Finley's theory of defense; and

- due to the conflicts of interests, none of the issues Mr. Finley has raised in this proceeding were raised on appeal, which denied him a first appeal as of right.

Finally, underlying Mr. Finley's Petition is his assertion that he is "actually innocent" of the charges. This claim is not a traditional claim of actual innocence, but is in fact a rephrasing of Mr. Finley's primary ineffectiveness claims. Although he asserts that he is in fact "actually innocent" of the charges against him, he bases this assertion on the same arguments supporting his ineffectiveness claims; that is, his trial and appellate counsel failed to competently and thoroughly investigate and pursue Mr. Finley's alternate remote user access defense. He claims

this resulted in the jury being denied the evidence upon which it would have found Mr. Finley to be innocent.

### A. Mr. Finley's Actual Innocence Claim and Remote User Access Theory

Mr. Finley's claim that he was actually innocent permeates his Petition and therefore the Court will first set out his allegations that someone else accessed his computers without his knowledge. As noted, this is not a typical claim of actual innocence. "To establish actual innocence, petitioner must demonstrate that, 'in light of all the evidence,' 'it is more likely than not that no reasonable juror would have convicted him.'" *Bousley v. United States*, 523 U.S. 614, 623 (1998) (*quoting Schlup v. Delo*, 513 U.S. 298, 327-328 (1995)). "'[A]ctual innocence' means factual innocence, not mere legal insufficiency." *Id.*

Mr. Finley acknowledges that he downloaded the GigaTribe software in early 2010, explaining that his intent was to use the program to share video games files and sessions, but that he "never bought into activate or register Gigatribe." Pet. Reply at 26 (ECF No. 136). He claims he did not activate the Boys4me2010 GigaTribe account, did not know that it was on his computer, and he was not the person operating the account. Similarly, he claims he was not the person who engaged in any of the numerous chat sessions with other GigaTribe users discussing receiving, distributing, and possessing child pornography using the Boys4me2010 account. Mr. Finley also claims that he was not the person who discussed with the undercover Agent and other users the user's desire to engage in unlawful sexual conduct with Mr. Finley's minor relatives. Finally, he claims he did not create the folders in the Boys4me2010 account named after his same minor relatives and containing images and videos of said children.

Mr. Finley's theory is that an unknown person unlawfully and surreptitiously gained remote access to his computer, and that the unauthorized user activated a GigaTribe account with

the username Boys4me2010 using Mr. Finley's birthdate and gender. This user then supposedly created several folders within the Boys4me2010 account including the primary folder titled "Stuff" as well as folders named after Mr. Finley's minor relatives. The remote user then proceeded to engage in unlawful activity involving child pornography from approximately August 2010 through December 2010. This user allegedly engaged in hundreds of chat sessions about child pornography with other users. In several of these conversations the user offered information directly aligning with Mr. Finley's life and relationships. The user downloaded over 30,000 unlawful child pornography files and placed them in folders on Mr. Finley's computer. Mr. Finley asserts that he did not know that this activity was occurring and did not know that the files were on his computer.

Mr. Finley acknowledges that the image of his minor relative on Mr. Finley's green couch, for which he was convicted of production of child pornography, was on his computer. He claims he is not responsible for distributing this file on GigaTribe. He otherwise does not address the existence of folders allegedly created by the unknown GigaTribe remote user titled with reference to his minor relatives or the fact that images of his minor relatives were placed in those folders.

Mr. Finley implies that the unauthorized hacking began with his old Compaq computer that was not connected to the Internet at the time of the search warrant. The Compaq computer did contain the Boy4me2010 GigaTribe account and the related folders containing over 30,000 files of child pornography as well as the folders and files related to his minor relatives. Mr. Finley explains that the child pornography files on his Dell computer were simply copied over from his old Compaq computer without his knowledge. Mr. Finley's admitted use of the Compaq computer and his subsequent copying over of files from that computer to his new Dell

computer occurred at the same time that the alleged remote user told his fellow GigaTribe users that he was in the process of transferring files from an old computer to a new computer.

Mr. Finley next claims without any evidentiary support that this "case reveals Petitioner the victim of multiple instances of anonymous, unauthorized user access activity; (*i.e.*, Hacker), resulting in the instant charges . . . ." Pet. Mot. To Vacate, at 7 (ECF No. 115). Mr. Finley supports his theory with evidence produced during the trial that when the search warrant was executed the Agents discovered the GigaTribe program up and running on Mr. Finley's computer when he was not at home.

Mr. Finley asserts that the "officers heard computer sounds coming from inside" and therefore entered his apartment in case evidence was being destroyed. *Id.* at 19. There is no evidence in the record that the officers heard computer sounds before entering the apartment. The evidence shows that at the time the search warrant was executed Agent Couch had logged onto GigaTribe and confirmed that the Boys4me2010 account was also logged onto GigaTribe. Tr. Jan. 24, 2012, at 8 (ECF No. 105). This information was relayed to Agent Shaffer who proceeded to execute the search warrant assuming that Mr. Finley was present in the apartment. *Id.* at 8-9. When no one responded to law enforcement's knock on the door the decision was made to forcefully enter the apartment in case Mr. Finley was attempting to destroy potential evidence. *Id.* at 9, 26-27.

Mr. Finley also erroneously asserts that the prosecutor implied Mr. Finley was at the apartment when the Agents arrived to execute the search warrant but left to go to his brother's house when he realized the Agents were there. *Id.* There is no evidence in the record to support this assertion. The evidence shows that after entering Mr. Finley's apartment and discovering

that Mr. Finley was not there, the Agents attempted to locate Mr. Finley, first by going to his brother's house, and then by calling Mr. Finley. Tr. Jan. 17, 2012, at 29-30 (ECF No. 92.)

The Government consistently maintained throughout the trial that Mr. Finley logged into GigaTribe as Boys4me2010 and left the program running for other users to access his files or to download his own files while he was not present at the computer. The Government presented abundant and consistent evidence that a feature of the GigaTribe file sharing network was that it allowed users to leave the GigaTribe program up and running to permit access for other users while not physically present at the computer. Thus, there was nothing unusual or suspicious about the fact that GigaTribe was running on Mr. Finley's computer when he was not at home.

Another flaw in Mr. Finley's theory is the presence of abundant evidence produced by the Government showing that in fact Boys4me2010 engaged in several conversations over several months with other users announcing that he will be absent from his computer and will leave his files accessible. In other conversations, Boys4me2010 apologized to users who had contacted him through his "up and running" GigaTribe account while he was absent from his computer.

Mr. Finley next points to the GigaTribe conversation between Boys4me2010 and PurpleTrim420, which shows that Boys4me2010 was communicating "via <thnks>," which Mr. Finley argues is indicative of abnormal user activity and unauthorized access. But Mr. Finley's assertion that a GigaTribe account using a nickname indicates abnormal activity is unsupported by the evidence. The evidence at trial showed that the user name or nickname THNKS was simply a nickname being used by the GigaTribe account Boys4me2010. Tr. Jan 19, 2012, at 93 (ECF No. 104).

In further support of his claim that his computer was "hacked" Mr. Finley offers evidence of a prior computer intrusion to his PNC Bank account. These allegations appear to be the evidentiary support Mr. Finley relies on for his alternate user defense theory as set out in detail in his Reply Brief. His theory is that this unauthorized access occurred through the use of a computer virus, perhaps "NETBUS" or "SUBSEVEN," but he argues that it could have been another virus. Mr. Finley claims that such a computer intrusion would have permitted the unauthorized user to gain control of his computer and perform the above activity related to the GigaTribe account without Mr. Finley ever being aware the activity occurred.

Mr. Patton did investigate the unauthorized activity regarding Mr. Finley's PNC Bank account, but was unable to find any evidence linking that activity to the remote user access of Mr. Finley's home computer. And, the unauthorized bank activity occurred on Mr. Finley's PNC Bank account, not on his home computer. The court understands Mr. Finley's assertion that it is perhaps possible that an unauthorized user first accessed his home computer in order to conduct the unauthorized bank activity, but Mr. Finley's assertions of such are wholly speculative. In addition, Mr. Finley's theory of various possible complex unseen computer hacking scenarios resulting in an intrusion into his computer by a user who proceeded to spend months primarily posing as Mr. Finley and using his computer to engage in the illegal conduct charged in the indictment is a completely unsupported speculative allegation.

The claims Mr. Finley raises in his 2255 Petition to support his claim of factual innocence are speculative, at best. The argument he offers to support his actual innocence claim is that his attorney should have pursued, in a different manner than he did, the theory that a remote user was the true perpetrator and therefore should have introduced *additional* evidence and witnesses in support of the theory. At best, Mr. Finley argues that had his counsel pursued

his theory differently than he did, it would have increased the likelihood that the jury might have believed that some unidentified "someone" other than Mr. Finley engaged in the charged conduct. He has not proffered any *evidence* to show that he is factually innocent, but instead merely proposes a variety of additional theories and arguments in support of the remote user defense his counsel had actually pursued at trial.[1] In contrast abundant evidence at trial overwhelmingly demonstrated that Mr. Finley was the user of the computer who engaged in the unlawful conduct.

Mr. Finley's theory that an unknown person surreptitiously hacked into his computer and engaged in months of continuous illegal conduct which Mr. Finley was not aware is also the foundation for the whole of Mr. Finley's 2255 Petition alleging ineffectiveness of counsel. As noted above, there are fundamental flaws in Mr. Finley's theory that he must overcome in claiming that he was actually innocent because his computer was hacked by someone else. Mr. Finley's theory also suffers from having to overcome the overwhelming circumstantial evidence supporting the conclusion that Mr. Finley in fact engaged in the unlawful conduct charged in the superseding indictment. For instance, there was factual evidence connecting Mr. Finley to the GigaTribe user account. And there were conversations that Boys4me2010 engaged in with other users revealing personal information consistent with evidence produced at trial regarding Mr. Finley's own life, including:

- the user having 4 minor relatives, with the exact names and ages of Mr. Finley's minor relatives;
- the minor relatives lived within a 7-block walking distance;

[1] For example, Mr. Finley asserts that counsel should have presented more specific evidence to establish how an unauthorized remote user connection might be established. But Mr. Patton did present a remote user access defense. He elicited testimony to show that a remote user could have accessed Mr. Finley's computer. The fact that he did not present the specific evidence in the manner Mr. Finley asserts he should have does not establish "actual innocence." It is merely an argument that more evidence (if any had existed) might have swayed the jury that a remote user did commit the crimes charged.

- the user referred to conduct he engaged in with a minor relative the same age as Mr. Finley's minor relative charged in the production of child pornography count;
- the user did not own a vehicle;
- the user announced that he was transferring his computer files to a new computer;
- the user was bisexual; and
- the user had previously been married.

And the username "Boys4me2010" was being used on Mr. Finley's computers for other programs such as Skype and AOL messenger.

Mr. Finley's theory depends, in part, on his assertion that he was completely unaware of the remote access user and thus also had to have been unaware of the folders the unknown user created. Weighing heavily against the theory that someone other than Mr. Finley surreptitiously engaged in this conduct is the time frame over which the illegal conduct occurred, the vast amount of digital files exchanged, and the time it would have taken to engage in the numerous chat sessions with other users all without Mr. Finley ever noticing the activity or content on his computer.

**B. Ineffectiveness Claims**

Were this 2255 Petition simply a claim of "actual innocence" it would be dismissed as implausible and speculative. However, Mr. Finley is not really claiming that he is "actually innocent;" his claim is that his counsel failed to pursue Mr. Finley's theory of defense in a manner, outlined by Mr. Finley in his pleadings, that would have better allowed the jury to conclude that Mr. Finley was not guilty. Because there was no direct evidence to show that Mr. Finley was physically present at the computer his remote user theory remains viable in his Petition. Therefore, the court will next address Mr. Finley's ineffectiveness claims.

"A claim of ineffective assistance requires a defendant to establish that counsel's representation fell below an objective standard of reasonableness and that the deficient performance prejudiced the defendant." *McAleese v. Mazurkiewicz*, 1 F.3d 159, 166 (3d Cir. 1993), *citing Strickland v. Washington*, 466 U.S. 668, 687-688 (1984). "The challenger's burden is to show that counsel made errors so serious that counsel was not functioning as the 'counsel' guaranteed the defendant by the Sixth Amendment.'" *Ross v. Dist. Att'y of the Cnty. of Allegh.*, 672 F.3d 198, 210 (3d Cir. 2012), (*quoting Harrington v. Richter*, 562 U.S. 86, 104 (2011)). "'[S]trategic choices made after thorough investigation of law and facts relevant to plausible options are virtually unchallengeable.'" *Hinton v. Alabama*, — U.S. —,134 S.Ct. 1081, 1088 (Feb. 24, 2014) (*quoting Strickland*, 466 U.S. at 690). "Because advocacy is an art and not a science, and because the adversary system requires deference to counsel's informed decisions, strategic choices must be respected . . . if they are based on professional judgment." *Strickland*, 466 U.S. at 681. "The Supreme Court directs that our 'scrutiny of counsel's performance must be highly deferential' to avoid holding counsel incompetent because of reasonable strategic or tactical judgments which, with the benefit of tactical hindsight, might prove not to have best served his client's interests." *United States v. Loughery*, 908 F.2d 1014, 1018 (D.C.Cir.1990), *quoting Strickland*, 466 U.S. at 689.

With respect to prejudice, a petitioner must "'show that there is a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different. A reasonable probability is a probability sufficient to undermine confidence in the outcome.'" *Hinton*, 134 S.Ct. at 1089 (*quoting Strickland*, 466 U.S. at 694); *see also Ross*, 672 F.3d at 210 (*quoting Richter*, 131 S.Ct. at 787).

Before addressing the specific ineffectiveness claims, the Court will review the actions taken by Mr. Patton regarding Mr. Finley's remote alternate user defense theory.

### 1. Counsel's Efforts Regarding Remote User Access Defense

Mr. Patton filed and won a motion to suppress statements Mr. Finley made the day the search warrant was executed. In winning that motion, Mr. Patton was able to exclude from trial Mr. Finley engaging in a nonverbal testimonial act that might well have been interpreted by the jury as an admission of guilt. Specifically, Mr. Finley was questioned about a video that was distributed from his computer's IP address that showed a minor child, previously identified by Mr. Finley as his relative, being fondled by an adult hand in Mr. Finley's apartment. In response to being questioned about this video Mr. Finley lowered his head and requested an attorney. This evidence was suppressed, but was information that Mr. Patton was aware of when developing a viable defense.

Prior to trial, Mr. Patton announced that he would be pursing an alternative perpetrator defense. Tr. Jan 18, 2012, at 3 (ECF No. 103). This was in response to the Government's pretrial preemptive motion in limine to preclude an alternative perpetrator defense. The Government argued that case law requires a defendant to provide a sufficient evidentiary nexus to show that another person committed the offense, and that a defendant cannot simply rely on speculation that it "could have been" someone else who committed the offenses. *Id.* at 2. Mr. Patton asserted he would rely on evidence introduced by the Government to argue "that someone other than Mr. Finley is engaging in this behavior." *Id.* at 3. Mr. Patton was permitted to pursue the defense subject to the Government seeking to preclude the defense at a later relevant juncture. At no time did the Court preclude Mr. Patton from pursuing an alternative perpetrator defense.

Prior to trial Mr. Patton investigated Mr. Finley's unauthorized remote alternate user defense. He employed a computer forensic expert from Carnegie Mellon University. The expert examined the computer evidence; however, Mr. Patton chose not to call the expert to testify at trial. *See* Def. Mot. in Limine, at 4 (ECF No.58). Mr. Patton filed a motion in limine to preclude the Government from mentioning the fact that the defense had hired a computer forensic expert but had chosen not to present testimony from the expert at trial. A reasonable assumption from these facts is that the expert was unable to support an unauthorized remote user defense, and Mr. Patton did not want the jury to make that assumption thereby weakening that defense. Mr. Patton was successful, as the Government indicated it had no intention of contending that the defense had hired a computer forensic expert.

During his opening statement, Mr. Patton explicitly announced to the jury that he intended to present the remote alternate user defense.

> We will prove to you in this case that while Craig Finley was not in his apartment at his computer someone was downloading images of child pornography on to that computer. And we will show you that while Craig Finley was not in his apartment someone was accessing that computer to make images of child pornography available to be shared using the GigaTribe software.
>
> We will prove that using the Government's own evidence. The Government's evidence will show you, in conjunction with records from Craig's employer, that while Craig was at work on multiple occasions someone used the computer in his home to download images of child pornography. On one occasion while Craig was at work someone accessed that computer and made images of child pornography available for sharing on the GigaTribe program.
>
> Now, I may not and probably won't be able to show to you who this person is, but the information that's stored on Craig's computer -- and we are going to talk about that in some more detail -- in conjunction with the records from his employer will show you that this happened. The evidence will show you that whoever this person is who was doing this is the person that is responsible for the child pornography activity that was occurring on Mr. Finley's computer.

Tr. Jan. 18, 2012, at 129-30 (ECF No. 103). Mr. Patton reiterated that "[o]bviously if Craig is at work, he's not putting files on his computer." *Id.* at 135. In noting that the evidence would show that someone was making child pornography shareable through GigaTribe on the involved computer that "[y]ou are going to see that this is being done, and it's being done in a time that it can't be Craig who's doing it." *Id.* Mr. Patton also indicated that the evidence will likely show that "there are programs, computer programs, that are available that will allow a person, one person using a computer to remotely access another computer." *Id.* at 135-36.

Mr. Patton also pursued the alternate user defense theory on cross-examination of several witnesses. He asked questions focused on the fact that no witness was able to testify that any person was actually sitting at the computer at the time the Boys4me2010 activity was occurring. He cross-examined Agent Botello along these lines as follows:

> Q. So it's fair to say that when you were communicating with whoever Boys4me2010 is, you could not see the person that you were interacting with, correct?
> A. That's correct.
> Q. You didn't use any kind of webcam to do a chat where you would actually see the person you're communicating with so that person sees you?
> A. Right.
> . . .
> Q. So basically what you end up with at the end of this is you know the IP address of the computer that you were connecting with through GigaTribe?
> A. Correct.
> Q. But you don't know who's at that computer?
> A. No.

Tr. Jan. 18, 2012, at 68, 69 (ECF No. 104).

Mr. Patton engaged in a similar inquiry with Agent Couch:

> Q. Agent Couch, when you're engaged in this GigaTribe undercover you are not able to see, physically see the person you are communicating with, correct?
> A. That is correct.
> Q. Now, so all you know is you know the name on the account, whatever they want to use, and using the other programs you can tell the IP address, correct?
> A. Correct.

*Id.* at 133-34 (ECF No. 104).

Mr. Patton also elicited testimony on cross-examination to support the alternate user theory by having witnesses agree that remote user access of a computer was possible, that a virus could infect a computer, and that unauthorized computer intrusions occur. In response to Mr. Patton's assertion that Agent Botello did not know if anybody was actually at the computer, Agent Botello said, "I would say somebody is at that computer because when I put in the request for the password, somebody typed in the password. So I would have to say somebody was at that computer in order to give the password." *Id.* at 69. Mr. Patton responded by questioning Agent Botello regarding the possibility of remote access to computers. *Id.* at 70. Agent Botello agreed that he was "familiar with computer programs that can be used to get remote access to another computer" and "there are programs where you could gain remote access to [a] computer from somewhere else." *Id.* This line of questioning ended as follows:

> Q. And so anybody that would be communicating with your computer that you are not physically sitting at, if they were running CommView, they would get the -- the IP address would come back to the computer you are remotely accessing because that's the computer that's going out to the Internet?
>
> A. I would say yes.

*Id.*

Mr. Patton cross-examined Agent Couch regarding remote user computer intrusions as follows:

> Q. When you say computer intrusions, you are talking about cases where some individual has gained unauthorized access to someone else's computer, correct?
> A. That's correct.
> Q. That can happen, there are people out there, they generally may be called hackers, right, that try to hack or break into other people's computers without authorization?
> A. Yes.
> . . .

Q. And you also do investigations of these people, hackers, sometimes they try and gain remote access to individuals' computers in attempts to get those individuals' computers to do things, correct?
A. Yes.
Q. Like are you familiar with the term, botnet?
A. I am, yes.
Q. A botnet is simply somebody, it could be somebody's personal computer sitting in their house that unbeknownst to them had been infected with a piece of malicious software, correct?
A. It could incorporate that possibly, yes.
Q. That allows, that malicious software allows someone else, this hacker from a remote location, to give this person's computer directions on what to do, is that right?
A. It could, yes.
. . .
Q. So what some of this -- these cases where you're investigating is people's computers have been infected with some type of software that can allow somebody else to gain access to their computer, correct?
A. The computer intrusion investigations, some of them, yes.

*Id.* at 134-36.

He asked Corporal Pearson about malware being placed on a person's computer:

Q. Yes. Now, you agree with me that there's this stuff called malware that's out there that's malicious software that can infect a person's computer?
A. Yes, sir.
Q. And make that -- can do just a whole host of different things to computers, correct?
A. Correct.

Tr. Jan 25, 2012, at 112 (ECF No. 106). He continued by cross-examining Corporal Pearson about remote user access occurring as a results of malware:

Q. There's also malicious software that will allow some remote -- some person other than the computer owner and operator to send directions to that computer to have that computer do things, like send out e-mails, spam e-mails?
A. Certainly, yes, sir.
Q. These are types of pieces of malware that if they get on to somebody's computer, it can allow somebody else to send commands to, for example, if I am the bad guy and if you have a computer sitting in your house, if I am able somehow to get the software on your computer, I am able to send commands to
18 your computer to have your computer e-mail?
A. Certainly.

*Id.* at 113. Mr. Patton directly asked Corporal Pearson if "there are pieces of software that allow a, what I will refer to as remote access to a computer," to which Corporal Pearson responded "Certainly, yes, sir." *Id.* at 114.

Mr. Patton also introduced documentary and testimonial evidence to show that Mr. Finley was at work during times when the computer evidence offered by the Government showed that GigaTribe activity was occurring. Tr. Jan. 25, 2012, at 146-56.

Finally, in his closing argument Mr. Patton stated:

> In my opening statement I told you that through the Government's evidence, by using the Government's evidence, we would show you that someone was using Craig's computer to download child pornography, move child pornography around on the computer, making it available for sharing while Craig was not home, while he was at work. That is exactly what we have done.

*Id.* at 198. Mr. Patton emphasized that computer access on Mr. Finley's computer occurred at a time when the evidence showed that Mr. Finley was at work. He explained to the jury that Mr. Finley's work records were the only evidence the defense had to show that Mr. Finley was not at home, stating "that's one thing we have that we can get our hands on, that we can then use to compare against the times that things are happening on the computers." *Id.* at 199; *see also* 203 ("we're comparing against the one thing we have that shows where Craig was for part of the time that these charges cover, and those are his work records.") Mr. Patton specifically argued from the evidence that this "is literally somebody taking images of child pornography, moving them on the computer, and making it shareable by GigaTribe while Craig is at work." *Id.* at 212. He argued to the jury that the only explanation is that "there's some malware" on the computer, and maybe someone who knows Mr. Finley "had access to Craig's apartment and put the malware or put some kind of program on the computer." *Id.* at 217-18.

The Court cannot say that Mr. Patton's representation of Mr. Finley fell below an objective standard of reasonableness or reveals errors so serious that counsel was not functioning as the counsel guaranteed the defendant by the Sixth Amendment. Mr. Patton investigated Mr. Finley's theory, and consistently pursued it from his opening statement through examination of witnesses to his closing argument. He vigorously pursued the remote user access defense as it was likely the only plausible defense available. Mr. Finley conceded that there was in fact child pornography on his computer that had been received and transmitted over the Internet. Mr. Finley's complaints about Mr. Patton's performance are in fact complaints aimed at Mr. Patton's informed strategic choices that are virtually unchallengeable. *Hinton*, 134 S.Ct. at 1088. The Court finds that Mr. Patton made reasonable strategic and tactical judgments based on his investigation and the evidentiary limitations he faced, and vigorously presented the remote alternate user theory to the jury.

### 2. Specific Ineffectiveness Claims

Having found that Mr. Patton's performance was not deficient with regard to the general pursuit of a remote user access defense, we will now address Mr. Finley specific claims of ineffectiveness.

#### *a. Failing to challenge the search warrant*

Mr. Finley claims that Mr. Patton was ineffective for failing to challenge the search warrant based on the allegation that the law enforcement officers knew before the search warrant was issued that there was remote unauthorized user activity on Mr. Finley's computer and therefore that he was not the sole suspect. The search warrant was supported by facts uncovered during the investigation that showed that an IP address for a computer located at Mr. Finley's residence was engaging in illegal conduct; specifically, the possession, receipt, and distribution

of child pornography. There is no evidence to indicate that the officers had knowledge that a remote user was accessing Mr. Finley's computer and chose not to disclose this information to the magistrate. Mr. Finley's theory is based on his erroneous assertion that Agent Couch's conversations with Boys4me2010 via the user name THNKS reflects abnormal or unauthorized user activity that should have alerted the officers. As explained, using a nickname or user name with an account on GigaTribe is not unusual. In addition, Agent Couch's conversation allowed him to ascertain that whoever was using the account divulged identifying information and activity indicating that the person was Mr. Finley.

Significantly, it does not matter whether the officers believed there was remote user access in this case, since probable cause existed to search Mr. Finley's residence based on the activity uncovered by the agents showing that the illegal conduct was occurring over an IP address located at Mr. Finley's residence. Therefore, had Mr. Patton challenged the search warrant on this basis, that challenge would have been unsuccessful. Mr. Patton was not ineffective for failing to raise such a meritless claim.

In his reply brief, Mr. Finley concedes that the officers initially had "probable cause to believe crime evidence existed at Finley's residence." Pet. Reply at 9. He then changes his argument to assert that after the officers entered the apartment and found the computer active probable cause was eliminated and the officers should have retreated and sought a new warrant. *Id.* at 9-10. There is no legal support for this proposition. Again, the evidence pointed to unlawful conduct on the computer located at Mr. Finley's residence. Once the warrant was executed, law enforcement properly seized the computers and questioned Mr. Finley.

### *b. Failing to move for acquittal*

Next, Mr. Finley argues that Mr. Patton was ineffective in failing to move for acquittal because the evidence did not prove the elements of production and receipt of the images, nor did the evidence establish that Mr. Finley was the recipient. Again, Mr. Finley's argument is based on the unsupported allegation that he was not the person who engaged in the conduct he was convicted of at trial. In other words, the argument is a reiteration of Mr. Finley's argument that the remote user engaged in the activity and his counsel was ineffective for not arguing for acquittal based on Mr. Finley not being the perpetrator. The evidence at trial was more than sufficient to establish beyond a reasonable doubt that Mr. Finley was the person responsible for the conduct. Moreover, Mr. Patton did move for acquittal as to Count One, arguing that a sleeping child cannot engage in sexually explicit conduct. This motion was denied at trial, re-raised on appeal, and its denial was affirmed.

### *c. Refusing to investigate or present an alternate user defense theory*

Mr. Patton did not refuse to investigate and present Mr. Finley's defense theory that an unauthorized remote user is responsible for the illegal conduct, so this argument is without merit.

### *d. Failing to subpoena character and fact witnesses*

Mr. Finley claims that Mr. Patton was ineffective for failing to call two character witnesses at trial. The first proposed witness, Mr. Finley's brother, allegedly would have testified that Mr. Finley routinely watched his brother's minor children, and that the children did not complain to the brother of abuse committed by Mr. Finley. The second proposed witness, a friend of Mr. Finley's, allegedly would have testified similarly that Mr. Finley stayed at his friend's home with his friend's children without complaints of abuse. He also claims ineffectiveness of counsel for failing to call his four minor relatives as fact witnesses to testify

that Mr. Finley did not abuse them, and a Children Youth Services case worker to testify that the minor children did not reveal sexual abuse allegations during Agency interviews.

The character evidence Mr. Finley claims should have been introduced is likely not admissible under Federal Rule of Evidence Rule 401(a)(1) as being irrelevant. In addition, the government correctly points out that whether Mr. Finley abused any of the minor children is not relevant to the crimes charged. Mr. Finley was not charged with sexually assaulting children; he was charged with production, receipt, distribution, and possession of child pornography. Mr. Finley concedes this point in his Reply. *Id.* Mr. Patton was not ineffective for failing to call such character witnesses.

Next, Mr. Finley claims that Mr. Patton should have called as fact witnesses a PNC Bank fraud representative; an Internet security and programming expert; and Mr. Finley's friend. Mr. Finley has not provided any evidence that these witnesses would have testified as he proffers, and asks the court to presume that he was prejudiced based on his own speculation. *See Duncan v. Morton*, 256 F.3d 189, 201 (3d Cir. 2001); *United States v. Gray*, 878 F.3d 702, 712 (3d Cir. 1989).

As noted above, Mr. Patton did investigate the unauthorized activity occurring on Mr. Finley's PNC Bank account. There is little connection between unauthorized activity occurring on Mr. Finley's third-party bank account and the charges in this case focused on Internet activity on Mr. Finley's personal computer, which were supported by abundant evidence. The Court cannot say that Mr. Patton was ineffective in choosing not to call a PNC Bank representative in such circumstances.

Mr. Patton did hire a computer forensic expert from a world-renowned university to examine Mr. Finley's computers but chose not to call him as a witness, presumably because he

had no testimony to support the remote user access theory. Mr. Finley concedes that the computer forensic expert's findings might have actually supported the Government's case against him, but asserts it is possible the evidence might have supported his defense. ECF No. 136, at 37. Given that Mr. Patton actively took action to make sure the Government was not able to tell the jury that the defense had hired a computer expert to examine the computers but chose not to have him testify, the Court cannot say that Mr. Patton was ineffective for failing to hire a different expert based purely on Mr. Finley's unsupported speculation that maybe the next expert's findings would be in his favor.

Finally, Mr. Finley alleges that his friend would have testified that he witnessed a user attempting to use Mr. Finley's username to obtain child pornography on other services and that the friend received suspicious emails purporting to be from Mr. Finley. But Mr. Finley concedes that he does not know if his friend would have been willing to or would have so testified at trial even if subpoenaed, as he has not spoken to him. ECF No. 136, at 37.

***e. Failing to adequately cross-examine government witnesses***

Next, Mr. Finley argues that Mr. Patton was ineffective for failing to adequately cross-examine government witnesses Shaffer, Couch, Botello, Pearson, and the mother of the minor relative involved in the production of child pornography count. For the reasons discussed above, Mr. Patton's cross-examination of the law enforcement witnesses was not only not ineffective, but quite on point.

Further, Mr. Patton's choice not to cross-examine the mother of the minor child did not fall below an objective standard of reasonableness. Mr. Finley claims that she would have testified that the child was a light sleeper who would have woken up if he was touched and that he did not complain of any abuse by Mr. Finley. Again, such evidence is irrelevant as the charge

was production of child pornography, not sexual assault. Moreover, the mother was understandably visibly upset and crying while testifying on direct examination and counsels' decision not to cross-examine her was tactically sound as there was likely no evidence in favor of Mr. Finley to be gained from her and the real risk of prejudicing his case before the jury.

### *f. Failing to object to prosecutorial misconduct*

Mr. Finley complains that Mr. Patton was ineffective for failing to object during closing argument to the prosecutor (i) referring to Mr. Finley as a "wolf in sheep's clothing, "and (ii) misrepresenting that Corporal Pearson knew that the child pornography files came from GigaTribe. "'[T]he appropriate inquiry [in deciding whether a prosecutor's remarks in summation require reversal] is whether such remarks, in the context of the entire trial, were sufficiently prejudicial to violate defendant's due process rights'" *United States v. Green*, 25 F.3d 206, 210 (3d Cir. 1994) (*quoting United States v. Scarfo*, 685 F.2d 842, 849 (3d Cir.1982)). The "prosecutor is entitled to considerable latitude in summation to argue the evidence and any reasonable inferences that can be drawn from that evidence." *Green*, 25 F.3d at 210.

The prosecutor's remarks here were a fair argument based on the evidence. The evidence showed that Mr. Finley took care of his minor relatives, treated them well and expressed concern for them at the same time that he harbored an ultimate goal of sexually abusing the children and obtaining unlawful images of them. Thus it was a fair characterization for the prosecutor to argue that Mr. Finley was a "wolf in sheep's clothing;" that is, someone who appears harmless while intending to cause harm.

The evidence also overwhelmingly indicated that the images of child pornography came over the Internet through the GigaTribe program, even if Corporal Pearson's actual testimony was that he could not definitively state where the images came from. Thus it was a reasonable

inference by the prosecutor to state that Corporal Pearson knew where the images came from. Finally, the Court sufficiently instructed the jury during opening and closing instructions that the attorneys' arguments are not evidence.[2]

### *g. Failing to be competent in computer forensics*

Mr. Patton engaged a computer forensic expert who examined the computers and produced a report. The Court's review of Mr. Patton's cross-examination of witnesses as well as his opening statement and closing argument demonstrates that he was competent and conversant in forensic computer issues for his purposes as trial counsel. Mr. Finley's claim that Mr. Patton was not competent is therefore unsupported, conclusory, and speculative.

### *h. Failing to preserve issues for appeal*

Mr. Finley's claim of trial counsel's ineffectiveness for failing to preserve issues for appeal is a redundant claim that Mr. Patton failed to pursue the remote user access theory of defense on the terms outlined in Mr. Finley's 2255 Petition. To the extent these claims were presented as ineffectiveness claims by Mr. Finley he was able to assert the claims in this Petition, and therefore he has not been prejudiced.

---

[2] Mr. Finley also argues that Mr. Patton should have objected during trial to the prosecutor's elicitation of uncharged allegations that Mr. Finley had engaged in inappropriate or unlawful sexual conduct with two minor relatives. Even if an objection had been lodged, such testimony was relevant and admissible as it confirmed that the GigaTribe user was in fact Mr. Finley. Recall that central to Mr. Finley's defense was that all of the computer-related conduct discovered by law enforcement was not perpetrated by Mr. Finley, but by some other as-yet-to-be-identified alternate user of Mr. Finley's computer. This evidence, ECF 104 at 108, 117-119, was plainly relevant to tie the computer-related conduct discovered by the FBI Agents as they were interacting on the GigaTribe network and related "chat" functions to Mr. Finley, and was therefore central to the Government's case as to the identity of the perpetrator. Thus, to the extent it would be considered "other bad acts" evidence, Fed. R. Evid. 404(b), it was properly offered to prove the identity of the person engaged in the unlawful child pornography activity, and further to rebut the essence of the defense that Mr. Finley offered then (and argues now), that (1) it was not, and could not, have been him, and (2) that he was not, and could not have been, the same person that the chats emanating from his computer demonstrated were from someone "interested in" children of their ages. ECF 106 at 167-68, 173, 182-188, 197. This evidence that tied the computer's real time user to Mr. Finley's nephews and therefore to Mr. Finley was plainly relevant for a permissible evidentiary purpose. Further, in consideration of the evidence of record as a whole, this Court is in no position to say that any prejudicial impact of that evidence so outweighed its probative value such that it had to be excluded under Fed. R. Evid. 403, particularly in light of all of the evidence of the actual child pornography that was admitted into the record, the admission of which was sustained on direct appeal. In light of those conclusions, this Court cannot say that defense counsel's failure to object to that evidence fell so far below (if below at all) the requisite standards of professional conduct applicable in assessing Mr. Finley's claims.

### C. Conflict of Interest/Conflicted Counsel Claims

Mr. Finley makes a vague claim that his right to effective counsel was violated by the Court denying his motion to appoint new counsel because it resulted in "conflicted" counsel. Specifically, he claims that trial counsel was "representing conflicting interests" because he refused to pursue Mr. Finley's defense in the manner Mr. Finley has outlined in his Petition. As noted above however, Mr. Patton in fact did pursue the defense competently. He was not successful primarily because the overwhelming evidence demonstrated that Mr. Finley was guilty.

Regarding the court's denial of Mr. Finley's motion to disqualify counsel, the Court held a hearing on the motion and after hearing from Mr. Finley *in camera* declined to replace Mr. Patton. At that time Mr. Finley complained that Mr. Patton was not following his direction as to the defense to be asserted and that he (Mr. Finley) was having trouble communicating with him (Mr. Patton). The "right to counsel does not include more than the right to representation by competent counsel at trial." *Siers v. Ryan*, 773 F.2d 37, 44 (3rd Cir. 1985). An indigent defendant who requests appointed counsel does not have an absolute right to appointed counsel of his own choosing. *Id.*, citing *Davis v. Stamler*, 650 F.2d 477, 479-80 (3d Cir.1981). In addition, "there is no corollary right to have any special rapport or even confidence in the court-appointed counsel." *Id.*, citing *Morris v. Slappy*, 461 U.S. 1, 13-14 (1983). The Supreme Court explicitly "reject[ed] the claim that the Sixth Amendment guarantees a 'meaningful relationship' between an accused and his counsel." *Morris*, 461 U.S. at 14.

Next, Mr. Finley claims that appellate counsel was ineffective because she was operating under a conflict based on the fact that she was employed by the same Federal Public Defender's office as Mr. Patton, that she failed to raise any issue based on Mr. Finley's theory of his

defense, and since the issues raised in this Petition were not raised on appeal, Mr. Finley was denied his first appeal as of right.

"Attorneys 'need not, and should not, raise every . . . claim but rather may select among them in order to maximize the likelihood of success on appeal.'" *United States v. Turner*, 677 F.3d 570, 577 (3d Cir. 2012) (*quoting Showers v. Beard*, 635 F.3d 625, 634 (3d Cir.2011) (citing *Smith v. Robbins*, 528 U.S. 259, 288 (2000)). Here, appellate counsel raised three issues on appeal: (1) whether the admission of explicit images of child pornography was proper in light of the defense's stipulation that they constituted child pornography, the images were prejudicial, and the trial court did not conduct an on-the-record weighing of the evidence; (2) whether a sleeping child can engage in sexually explicit conduct; and (3) whether the Court's sentencing determinations and considerations violated the Double Jeopardy clause. Mr. Finley is unable to show that the result of his appeal would have been different had appellate counsel chosen to raise the issues he now claims in his 2255 Petition. *United States v. Mannino*, 212 F.3d 835, 845 (3d Cir. 2000).

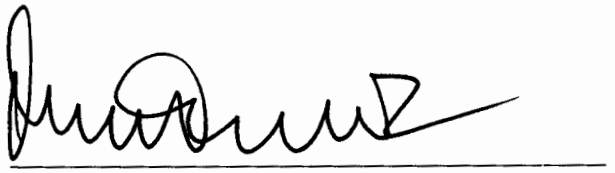
**D. Certificate Of Appealability**

No certificate of appealability should issue in this case. A court should issue a certificate of appealability where a petitioner makes a substantial showing of the denial of a constitutional right. 28 U.S.C. 2253(c)(2). A petitioner meets this burden by showing that reasonable jurists would find the district court's assessment of the constitutional claims debatable or wrong. Slack v. McDaniel, 529 U.S. 473, 484, 120 S.Ct. 1595 (2000). We find that jurists of reason would not find it debatable whether Mr. Finley states a valid claim of the denial of a constitutional right and jurists of reason would not find it debatable whether this Court was correct in concluding that the

Petition does not present any claims upon which relief may be granted. Therefore, the Court will deny a certificate of appealability.

## IV. CONCLUSION

Having found no merit to Mr. Finley's claims of ineffectiveness of counsel and related claims that he is actually innocent based on an unknown, unauthorized remote user theory, Mr. Finley's Motion to Vacate, Set Aside, or Correct a Sentence pursuant to 28 U.S.C. § 2255 will be denied.



Mark R. Hornak
United States District Judge

Dated: August 15, 2017

cc: All counsel of record